CLAIMS

1. A user identification information protection method for encrypting each field of a message transmitted through at least one relay station by using encryption schemes which are respectively effective in between a relay station requiring each field or a party on the other end of communication.

2. The user identification information protection method according to claim 1, comprising the steps of:

encrypting a part of the message containing identification information of a mobile user by using an encryption scheme which is effective in between the party on the other end of communication; and

encrypting a remaining part of the message by using an encryption scheme which is effective in between the relay station.

3. The user identification information protection method according to claim 1, comprising:

a first step of encrypting a part of the message containing identification information of a mobile user by using an encryption scheme which is derived from subscription information of the mobile user; and

a second step of further encrypting the message

subjected to encryption in the first step by using an encryption scheme which is effective in between the party on the other end of communication.

4. A user identification information protection method comprising the steps of:

performing hierarchical encryption of each part of a message containing identification information of a mobile user with keys at different encryption levels respectively;

routing the encrypted message to a correct network by using a home domain name; and

further concealing actual identification information of the mobile user by using a temporary domain specific identifier.

5. The user identification information protection method according to claim 4, further comprising the steps of:

protecting the identification information of the mobile user having an intended receiver's key by using asymmetric cryptography; and

protecting the identification information against attacks from a third party by using a challenge message - response exchange scheme for a mutual authentication of a mobile terminal and a network.

6. The user identification information protection method according to claim 5, further comprising the steps of:

sharing the intended receiver's asymmetric cryptography key with the mobile terminal prior to a start of message exchanges and storing the asymmetric cryptography key in a storage device that could be accessed by the mobile terminal securely;

updating the asymmetric cryptography key pair by including a new asymmetric cryptography key in a replied message encrypted by the current asymmetric cryptography key; and

identifying the asymmetric cryptography key pair currently used in the encryption for the identification information protection by embedding information in domain information.

7. The user identification information protection method according to claim 4, wherein a message sequence is capable of mutually authenticating the mobile terminal belonging to WLAN and its home network in one message round trip, wherein the method comprising the steps of, through the message sequence:

the mobile terminal sending to the access point the encrypted identification information, mutual

authentication information, mobile user home domain information, and other necessary information;

the access point sending to a mobile user's home domain server the encrypted mobile user identification information, the mutual authentication information, and other necessary information by using the mobile user home domain information;

the access point receiving from the mobile user's home domain server the mutual authentication information and other information; and

the mobile terminal receiving from the access point the mutual authentication information and other information forwarded by the access point from other server.

8. The user identification information protection method according to claim 7, comprising the steps of, through the message sequence:

the mobile user's home domain server sending to the central server a message comprising the mutual authentication information and other information forwarded by the access point from mobile terminal; and

the mobile user's home domain server receiving from the central server the message comprising the mutual authentication information and other information to be forwarded to the mobile terminal.

9. The user identification information protection method according to claim 7, wherein a set of message format to be used in the message sequence comprises:

mobile user identification information specific to the WLAN accessible to all network nodes;

mobile user's home domain information accessible to all network nodes;

mobile user's credential and identification information hierarchically encrypted and only accessible by the intended receiver;

an authentication challenge message and response encrypted and only accessible by parties involved in the mutual authentication; and

information for message integrity protection.

10. The user identification information protection method according to claim 9, wherein the message format further comprising:

information for identifying a key used for the hierarchical encryption to the intended receiver; and

information for generating a new key for protection of the identification information.

11. The user identification information protection method according to claim 7, comprising the steps of:

deploying one or more virtual terminal that is able to access the user's credential and subscription information and carries out the inter-working function as a normal mobile terminal from the inter-worked network;

using as a gateway for a WLAN device associated with the virtual terminal to access services provided by the inter-worked network; and

controlling the service access of the WLAN device to the inter-worked network by the virtual terminal.

12. The user identification information protection method according to claim 11, comprising the steps of: accessing one or more of the users' credential and subscription information simultaneously by the virtual terminal; and

sharing these one or more users' subscribed services from the inter-worked network in WLAN.